planet DDS | dentalOS®

DentalOS & DentalOS Admin Field Guide

INTERNAL USE ONLY

Contents

01. Overview 3

Feature summary 3

Commercial structure 3

02. Setup 3

Internal configuration 3

Validating an organization 3

Editing an organization 4

Creating super admins 6

Product-specific enablement 9

Customer access 11

Prerequisites 11

03. Getting started 12

User interface 12

Home 12

04. Use cases 13

Internal administration 13

Audit log 14

Migrations 15

Organization management 17

User management 18

Account recovery 19

Security policy management 20

User authentication 21

IP allowlist 22

Organization administration 22

Audit log 23

General workflows 24

Customer onboarding 24

Super admin tasks 24

05. Troubleshooting 24
Frequently asked questions 25
06. Appendix 26
Other resources 26
Revisions 26

01. Overview

Feature summary

DentalOS is a dental enterprise platform unifying Planet DDS products such as Denticon and Cloud 9 within a single data layer. Users can rely on single sign-on to launch products, manage users, and configure security policies.

Specific platform capabilities include:

- Role-based permissions
- Centralized hub featuring products, metrics, and resources of the customer organization
- Organization-wide security controls, including multi-factor authentication, Entra ID single sign-on, IP policies, and account recovery protocols
- An audit log to review system activity in DentalOS

Key value drivers

For large DSOs with complex organizational needs, DentalOS reduces friction and drives efficiency where administrative control and product visibility is concerned. Organizations of any size can realize these same benefits.

DentalOS not only provides value to DSO owners and executives, but offers scalable access governance to IT staff and system admins, office managers, and dentists.

Commercial structure

Product SKU	51000 (DentalOS)
Product details	Core

02. Setup

Internal configuration

Implementation Coordinators will be responsible for configuring accounts for new and existing users. The process for adding new organizations is explained below.

Onboarding existing customers involves more complexity due to syncing customer data from existing practice management systems (PMS) into DentalOS.

Validating an organization

Organizations are created automatically in **DentalOS Admin** using **Salesforce** information. Implementation Coordinators must ensure that each organization's details, products, and org groups match the customer's Salesforce account and Closed Won opportunity.

A key term in navigating DentalOS is organization groups or org groups. Org groups are location groupings used to associate products, accounts, or offices within an organization.

Implementation should create at least one org group per product account for the customer organization to ensure proper data syncing. For example, during initial setup, Implementation should create one org group per Denticon PGID or Cloud 9 URL.

Access **DentalOS Admin** via the following web address: dos-admin.mydentalos.io. Use your Planet DDS login. Ensure you're on the **Organizations** tab.

Open **Salesforce**. If necessary, use a split screen to view both **DentalOS Admin** and **Salesforce** simultaneously.

For detailed steps and screenshots, review the **DentalOS Admin + Salesforce** video walkthrough and/or the **DentalOS Admin + Salesforce: Account & Product Setup Guide**. Both are included in the **Appendix** on the last page.

When validating, note the following:

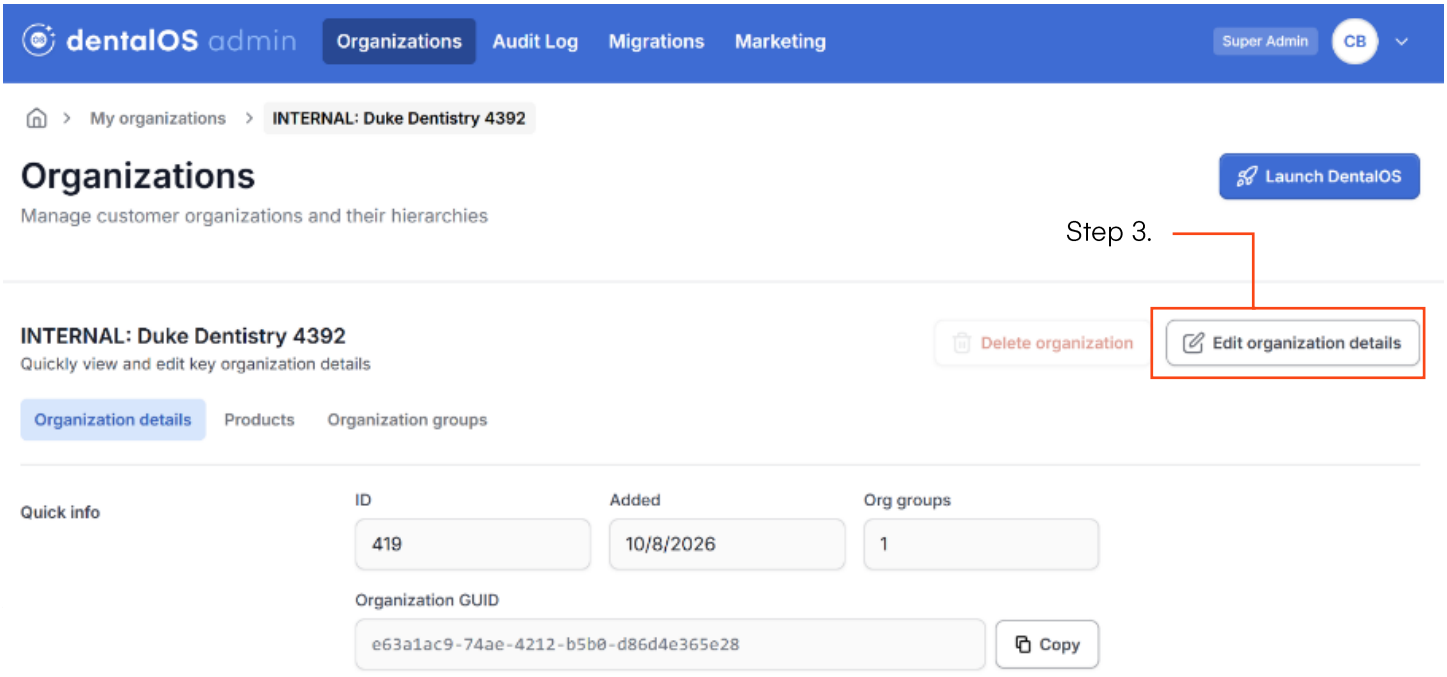
- Recording the wrong number of locations will adversely affect the customers' ability to access their system, potentially leading to a billing error
- For **Cloud 9** org groups, the Account field should contain only the tenant subdomain, not the full [tenant].cloud9ortho.com address.
- For organizations that use both **Denticon** and **Cloud 9**, an account should be assigned for every PGID and URL.

The Salesforce automation creates organizations and org groups, in addition to enabling products per location, but it does not enable products at the org group level. This must occur manually by editing an organization.

The established resources above review this process. The steps below delineate the navigation path for making edits.

Editing an organization

Use the following steps to enable products as well as correct any discrepancies identified during validation.



Step 2. Click on an organization to edit key details.

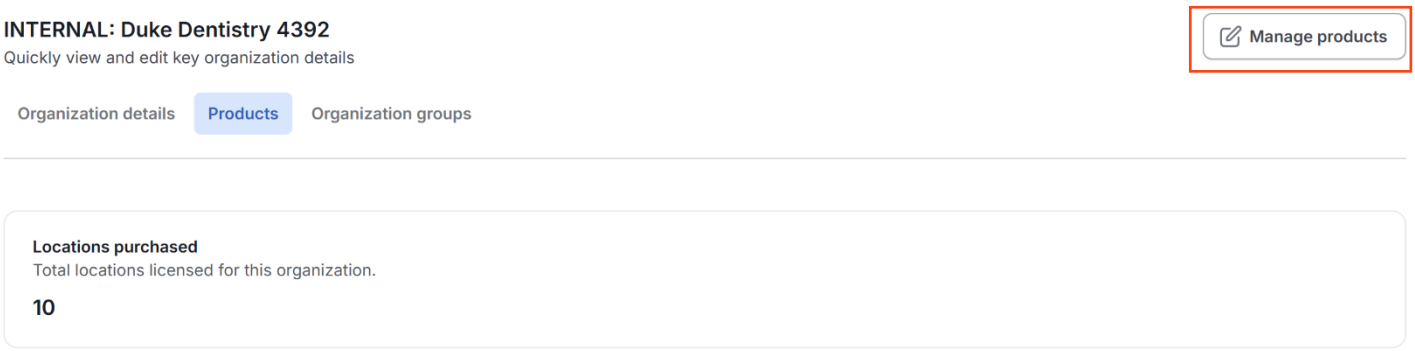
Step 3. In the **Organization details** tab, you will see the information imported from Salesforce for validation.

Click **Edit organization details** to edit details such as the organization name, address and primary contact.

Step 4. In the **Products** tab, you should see the total locations licensed for the organization and the organization's core products, add-on suites, and add-ons.

This information is imported from Salesforce, but should be validated.

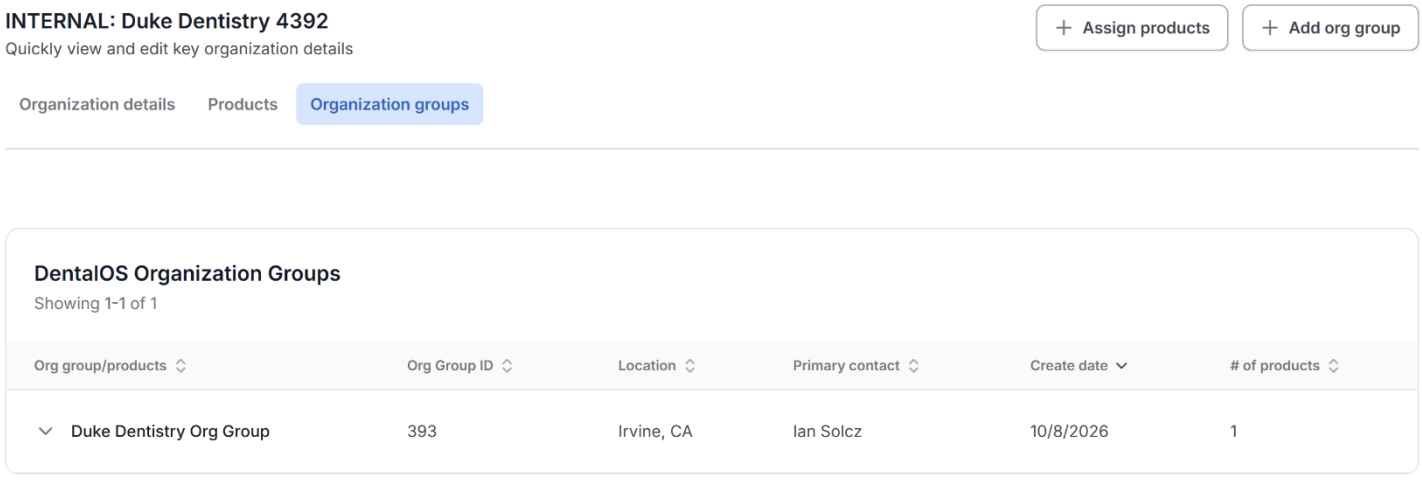
Click **Manage products** to edit details such as locations purchased and enabled core products, add-on suites, and add-ons.



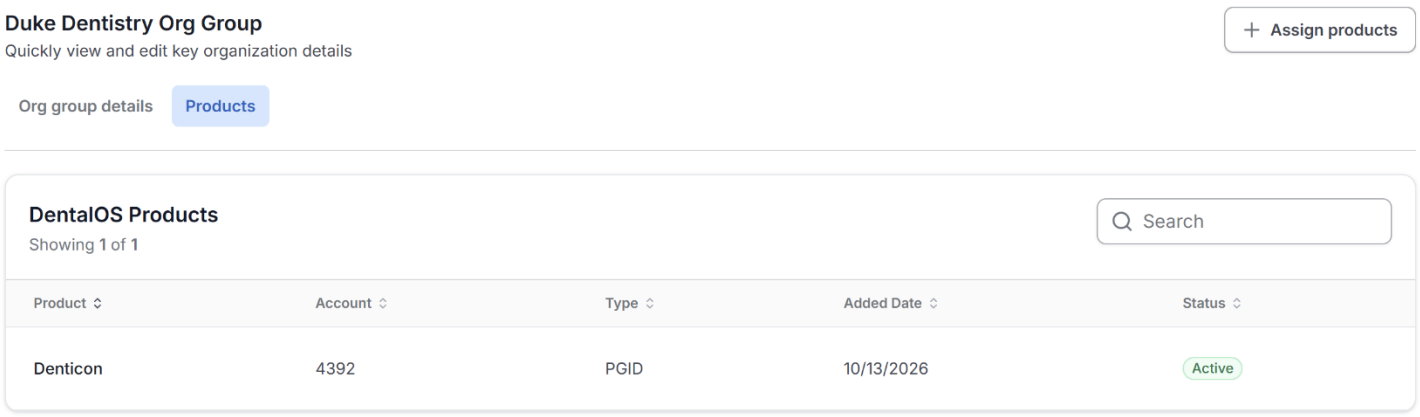
Step 5. In the **Organization groups** tab, you should see the org groups that that belong to the organization. Use Salesforce to validate this information.

Step 6. Click **Add org group** to add additional org groups.

For an organization that utilizes **Denticon** and **Cloud 9** products, it is recommended to assign an account for every PGID and URL.



Step 7. To assign products, click directly on the org group name, then select the **Products** tab, and finally **Assign products**.

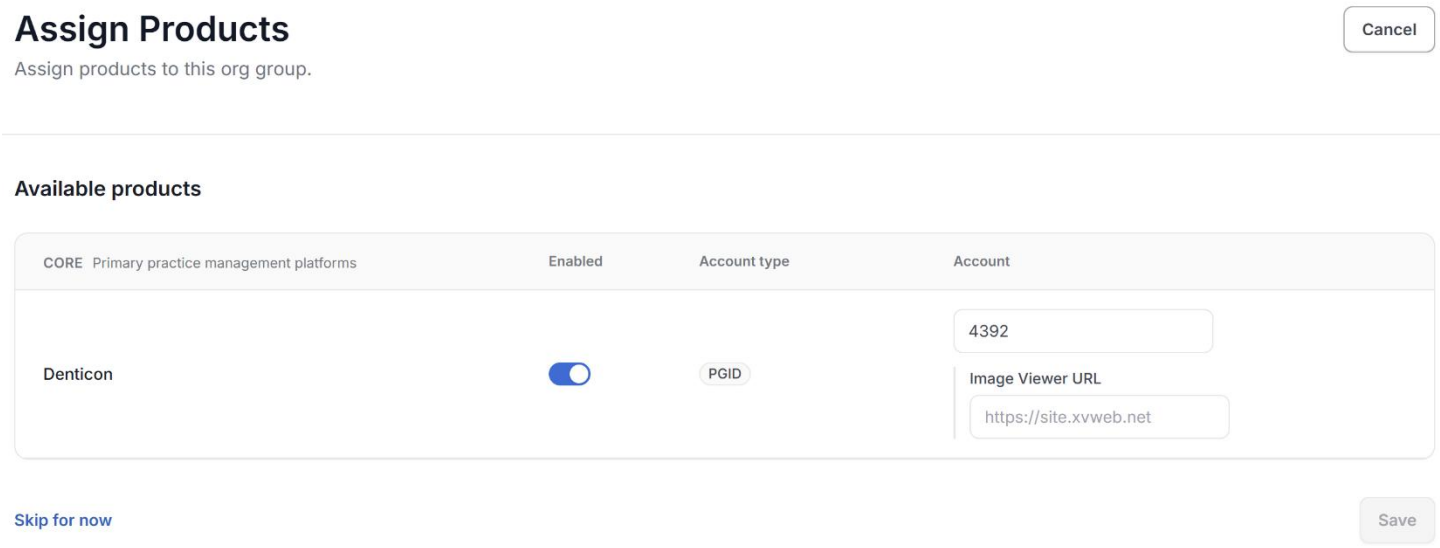


Step 8. Enable products, add-on suites, and add-ons as they relate to the customer's sales quote.

Step 9. On the right-hand side, enter information that correlates with the specified **Account type** field on the same page.

Do not enter text that does not abide by the cited type. For example, enabling the **Cloud 9** core product requires entering a subdomain. Rather than entering the full web address for an account as [tenant].cloud9ortho.com, only enter the tenant part of the URL.

Click **Save** once finished.

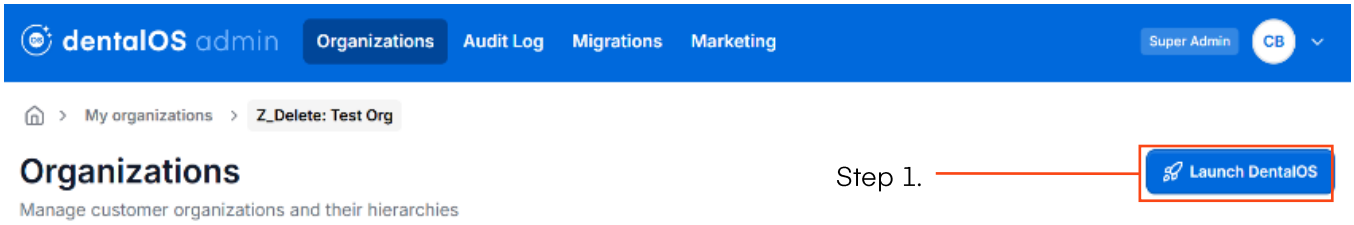


For a visual aid related to these tasks, refer to the video and guide referenced above.

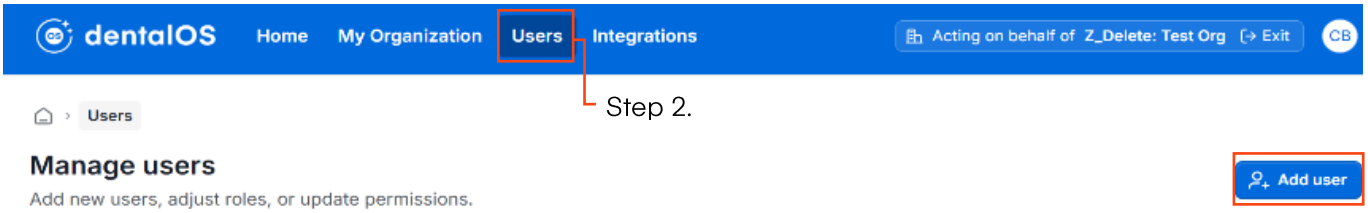
Creating super admins

Create two Super admin accounts for each new organization. The first is typically the organization's executive owner, such as the CEO. The second should be an authorized administrator who is equipped to take on operational tasks such as adding users and assigning locations.

Step 1. Inside **DentalOS Admin** on the **Organizations** tab, select an organization, then **Launch DentalOS** on the top right.



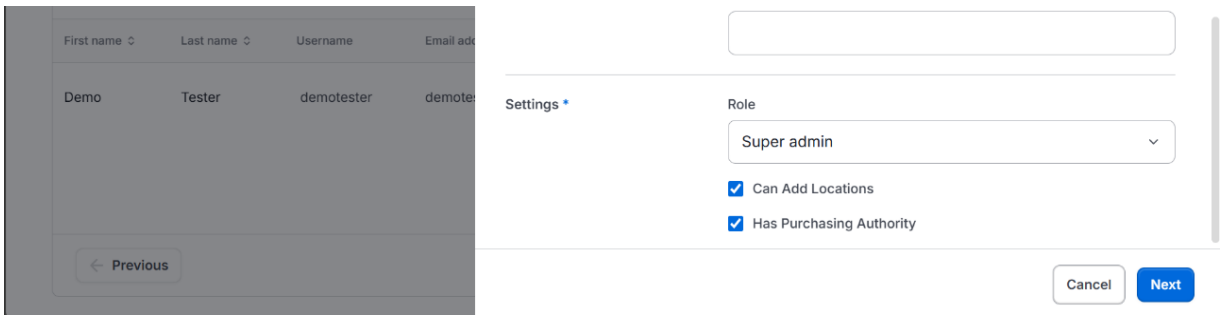
Step 2. In the resulting interface, select **Users** → **Add user**.



Step 3. Add user information as prompted. Entering a phone number will aid account recovery but it is not required. Email is only required if SSO is enabled. In this case, the username and email address must be the same.

Step 4. In the final **Settings** field, set the **Role** as **Super admin** to give the account full administrative rights. Super admins will then be able to configure locations, additional users, and security settings.

The checkboxes adjacent to **Has Purchasing Authority** and **Can Add Locations** can be selected for any user role, regardless of other privileges, but they must be checked for the Super admin account. The **Has Purchasing Authority** selection allows the user to manage agents.

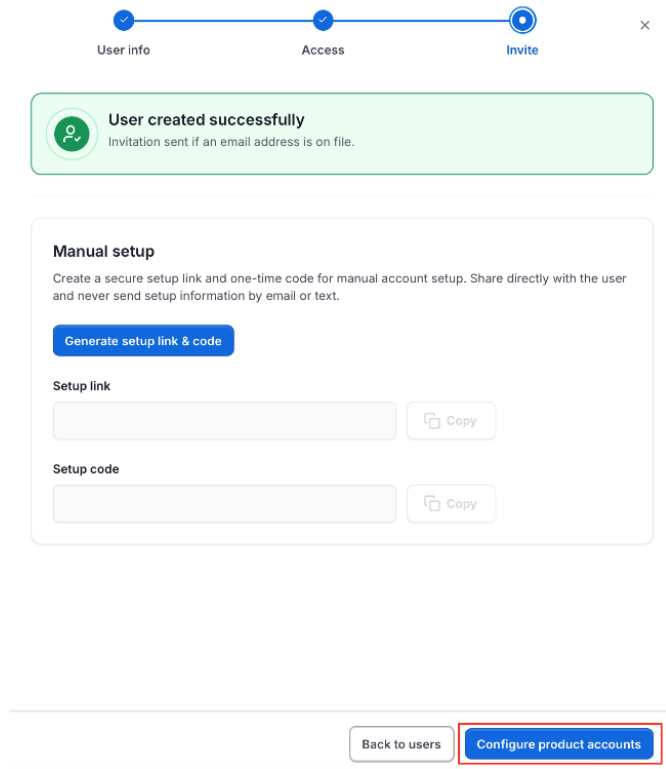


Step 5. Click **Next** to proceed. Super admins will automatically be given access to all locations, bypassing the **Access** step.

If the user provides an email address, an invitation will be sent to the address on file if one exists. The user has 24 hours to accept their invite.

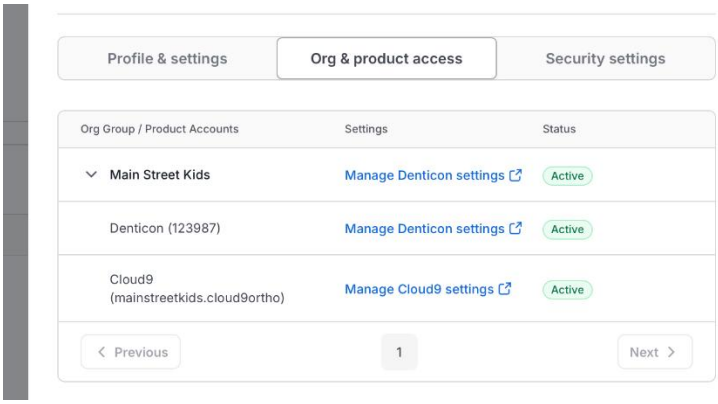
Step 6. If the user does not provide an email address for the Super admin account, they must click **Send invite** on the bottom right of the page that appears.

Step 7. Click the **Generate setup link & code** button on the screen that follows. The link and code that appears must be shared directly with the account user. Then click **Configure product accounts.**



Step 8. The resulting screen will show the organization to which the user is attached and the products they can access. On the right, a link or multiple links will appear to manage each product's settings (e.g., **Manage Denticon settings**). Use the links to assign users permissions within each product account.

Permissions do not have to be set in Apteryx.

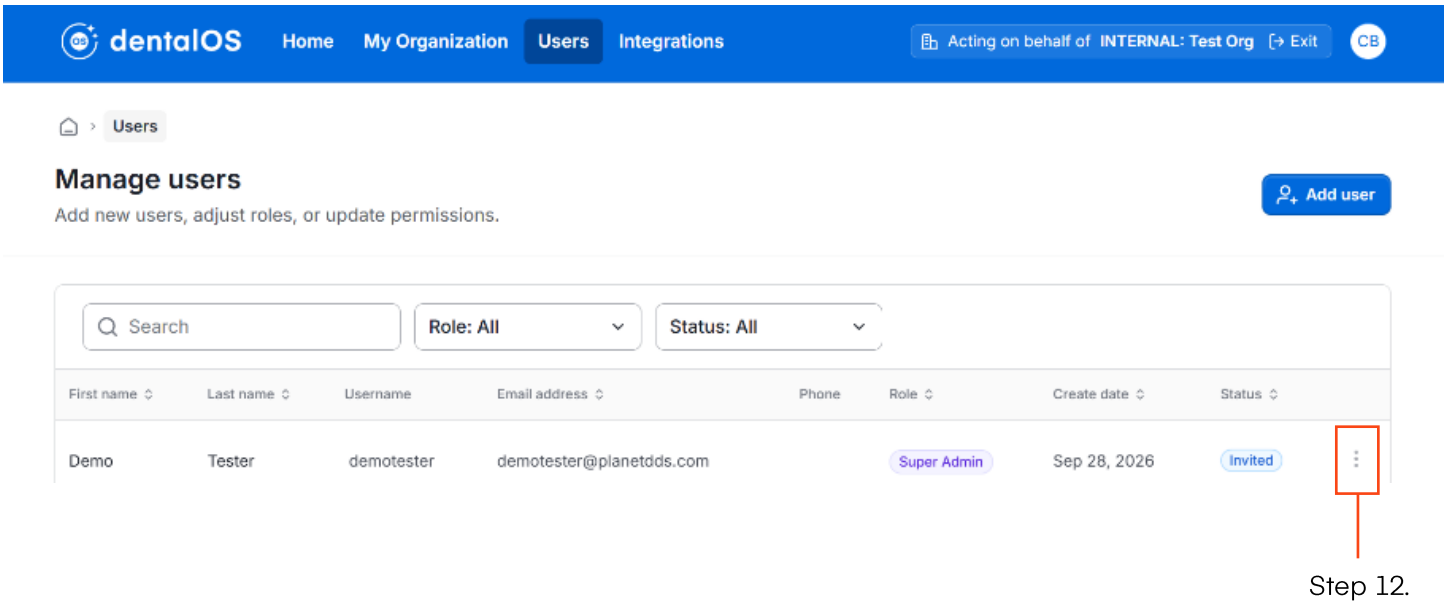


Step 9. In **Denticon**, select **Setup → Security**. Search for and select the name of the relevant Super admin. Then select **GROUP MEMBERSHIPS → EDIT USER**, and assign the appropriate user groups. To do this, select a user group from **Available User Groups** and then click the right chevron. Click **Save**.

Then select the **USER SETTINGS**, **EDIT USER**, and select the appropriate role for the account user in the **User role/type** field. Click **Save**.

Step 10. In **Cloud 9**, select **Edit → Setup → Employees**. Search for and select the name of the relevant Super admin. To the right of the **Edit Employee** pop-up that appears, use the **Permission** box to select appropriate permissions.

Step 11. Repeat steps 2-10 to create a second Super admin.

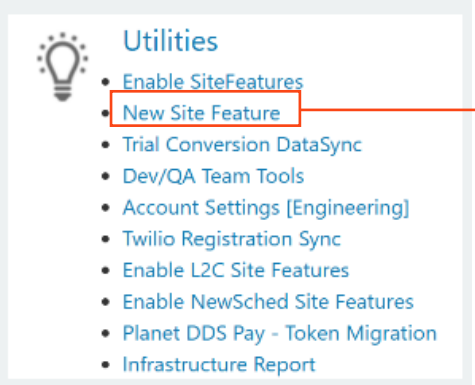


Product-specific enablement

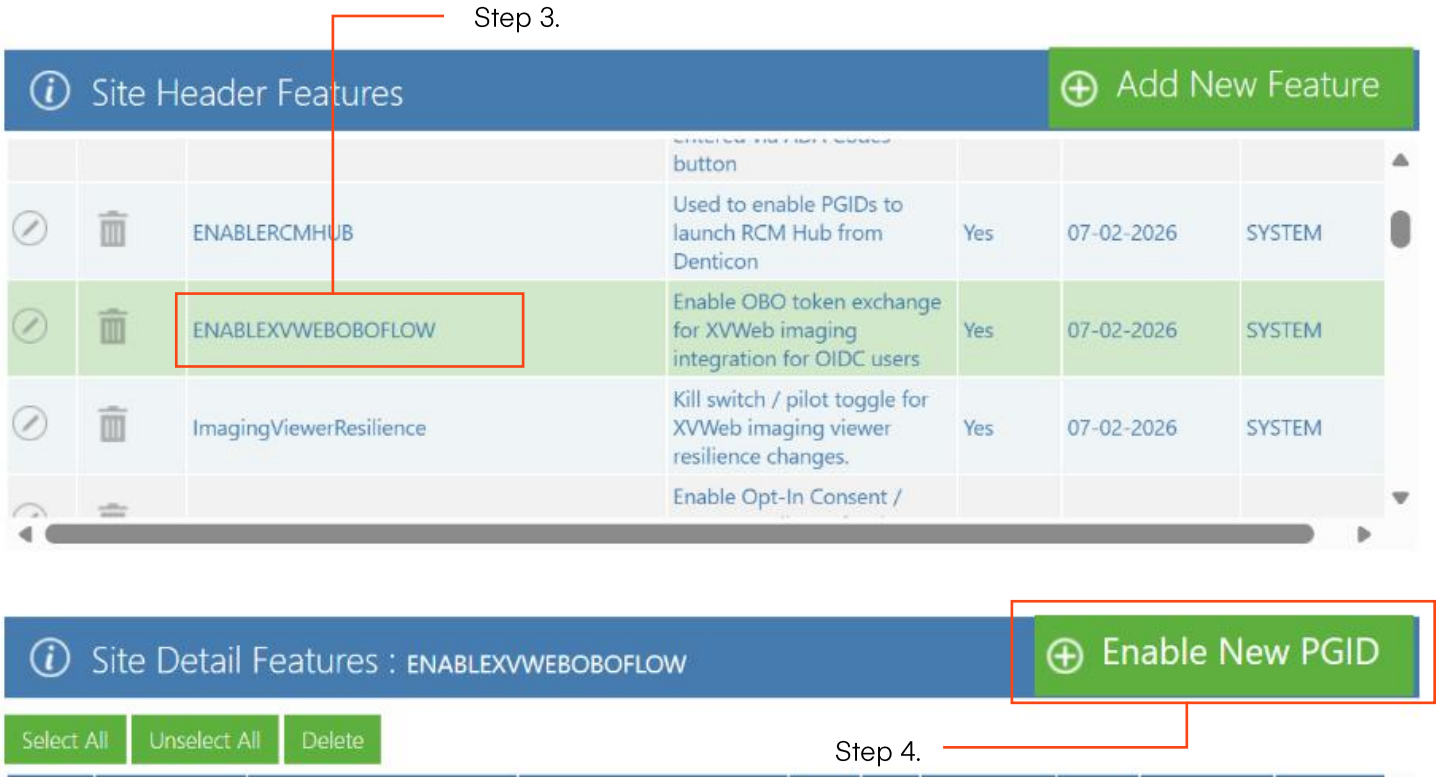
For **Apteryx** and **Denticon**, site features must be enabled for net-new customers.

Step 1. Go to the **Denticon Administration Panel** portal.

Step 2. Click the **New Site Feature** link in the **Utilities** panel.

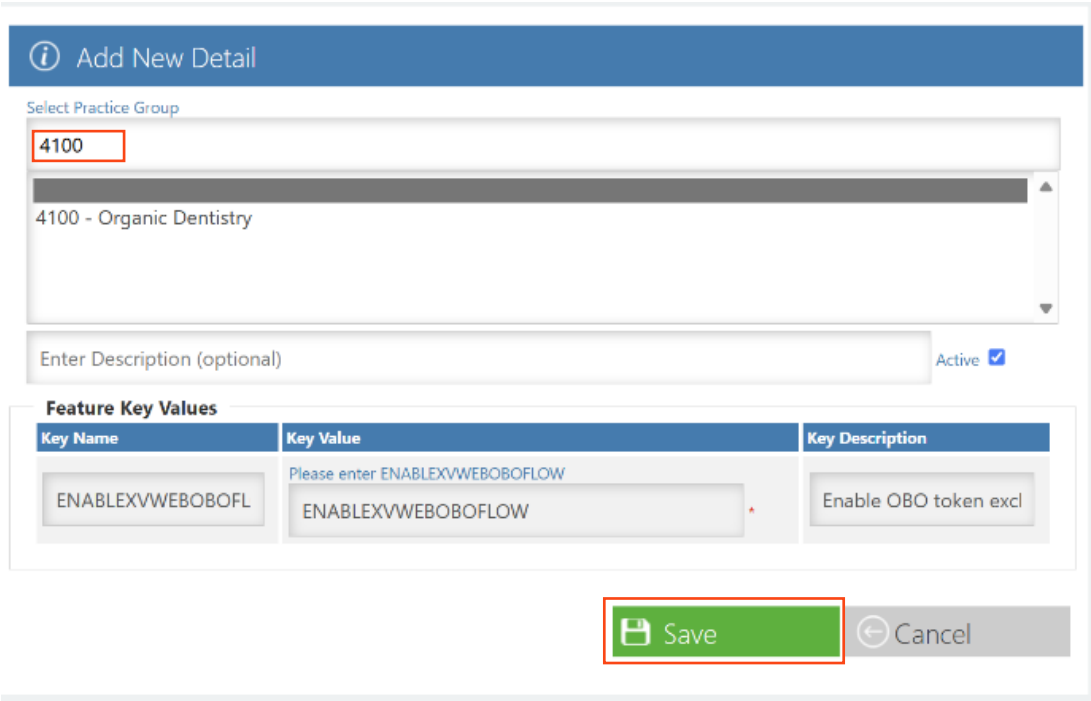


Step 3. Select **ENABLEXVWEBOBOFLOW** from the **Site Header Features** section.



Step 4. Click **Enable New PGID** from the **Site Detail Features** section.

Step 5. Enter the PGID of the new customer, select their practice group, and click **Save**.

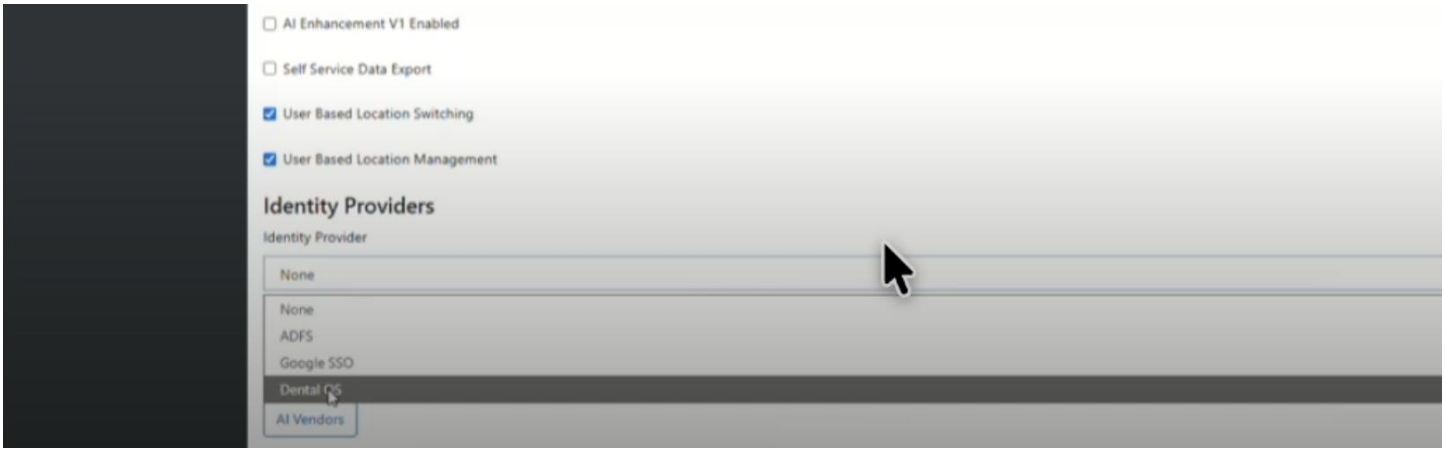


Step 6. Select the **Back** button to return to **Site Header Features**, and enable the following flags for the customer's PGID using the same process illustrated in steps 3-5:

- ENABLE_TOPNAV_SECONDARY
- ENABLE_TOPNAV_PRIMARY
- ENABLENEWTOPNAVIGATION.

You will only be able to enable one flag at a time.

Step 7. In **XVWeb Admin**, navigate to **Sites**, then **Identity Providers**. Set **DentalOS** as Identity Provider in the corresponding site.



Customer access

Existing customers must reach out to their Customer Success Manager to learn about moving to DentalOS. However, in coming months, customers will no longer have the option to opt in or out. Planet DDS will schedule each customer's onboarding date and notify them in advance.

For new customers, the process starts after Implementation sets up the initial Super admins. Each user receives an email invitation or a one-time setup code.

After creating a password, the Super admins can sign in to DentalOS and configure security policies, create locations, add users, and assign roles, locations, and product access.

DentalOS automatically creates users in the product accounts to which they are assigned. Granular product-specific permissions are then configured in the applicable core product.

Users should sign in through the DentalOS URL and launch their assigned products from the DentalOS home screen.

Customer access DentalOS via dos-app.mydentalos.io.

Prerequisites

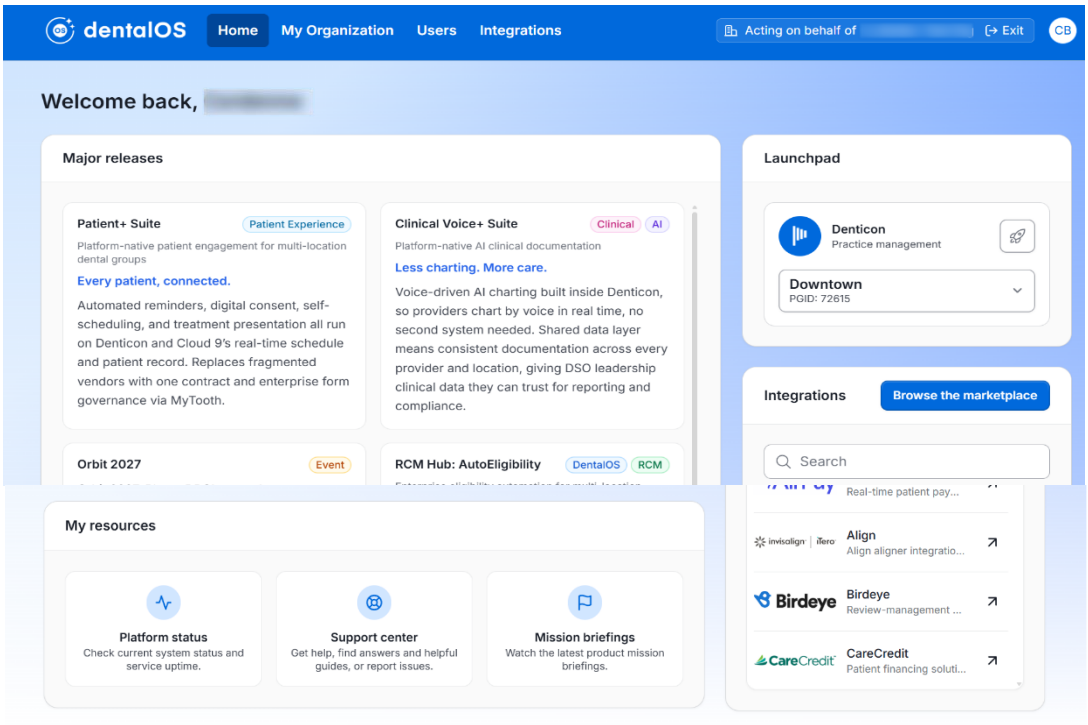
- Pop-ups allowed for Apteryx
- Feature flags for MFA and SSO must be enabled at the PGID/Database level before IT Admins can configure security policies in Denticon and Cloud 9

03. Getting started

Customers access DentalOS at dos-app.mydentalos.io. The **Home** page features several panels and navigation tabs that users can employ to manage their organization.

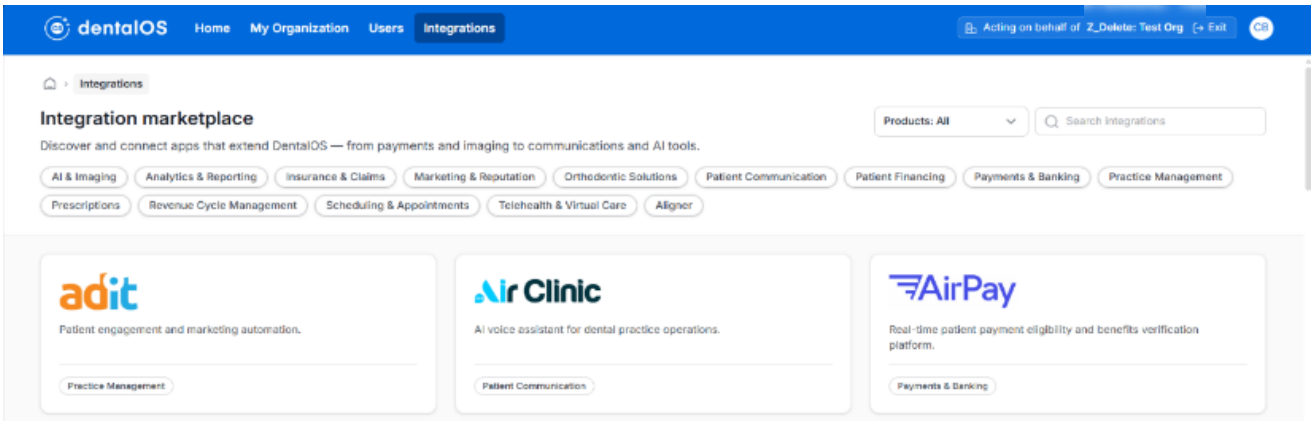
User interface

Home

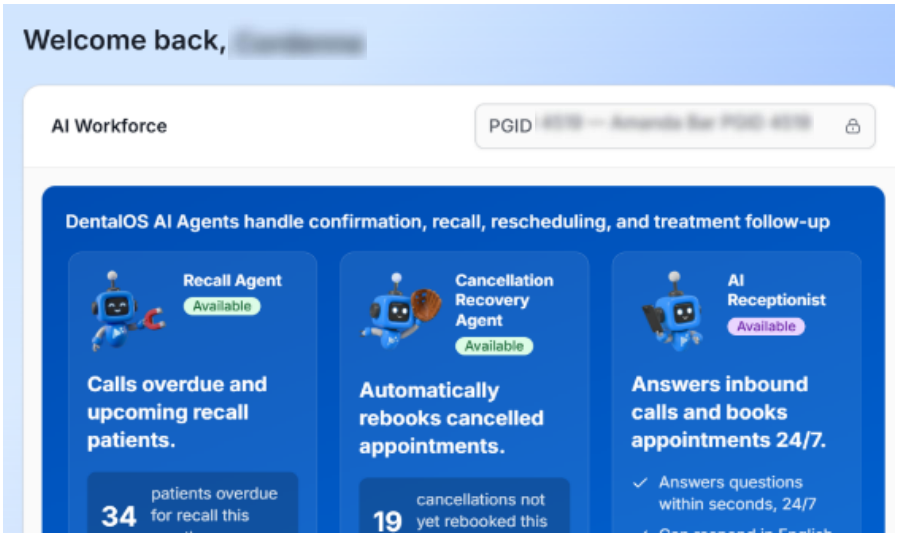


- The **Launchpad** panel provides a central location for users to launch and access their Planet DDS products; to launch a product, users should click the rocket ship icon ( ) to the right of the product name to launch their desired product
- **Major releases** highlights significant product updates and featured events
- The **Integrations** panel on the **Home** page features a short preview of available integrations that connect DentalOS with other products and services

  Clicking **Browse the marketplace** opens the **Integrations** tab which features a comprehensive marketplace of vendors.



- **My resources** provide quick access to organizational resources such as the support center and system status
- All customers have **AI Workforce** enabled, but only users with **Has Purchasing Authority** privileges can see the panel as well as the **Agents** tab



This panel features AI Agents that are available for purchase. If any agents are active, a small panel above labeled **Active agents** will show live agents and indicate whether the customer is in a trial or paused.

Agent-related data like ROI will also be returned in the same panel.

The dashboard header is role-aware. If the user is a super admin or group admin, it shows **My Organization**, **Users**, and **Integrations**. **Agents** are shown for any user with purchasing authority.

If the user has the role **User**, they can only see the **Home** page unless specified privileges determine otherwise. Super admins can also control which panels users see on the **Home** page.

Users must log into **DentalOS** to access Planet DDS products. However, users can choose whether their initial landing page is **DentalOS** or a specific product by clicking their profile icon, then **View profile** on the **Home** page. Super admins can also configure the landing page for other users within their organization.

The other available tabs will be illustrated in Use cases.

04. Use cases

Internal administration

For internal teams, the most substantial shift DentalOS brings is DentalOS Admin. DentalOS Admin allows internal Planet DDS users to manage organizations on their behalf, edit organization details, and migrate existing customers.

However, these privileges do not exist for every internal user and the extent of these privileges differ by roles. Refer to the table to learn more about internal roles in DentalOS.

Capability	Super Admin	Onboarding	Support	Marketing
Sign in via Entra SSO	✓	✓	✓	✓
Create Organization	✓	✓	X	X
Edit Organization	✓	✓	✓ (non-destructive only)	X
Delete Organization	✓	X	X	X
Create Org Group	✓	✓	X	X
Edit Org Group	✓	✓	✓ (non-destructive only)	X
Delete Org Group	✓	X	X	X
Add Product association	✓	✓	X	X
Delete Product association	✓	✓	X	X
Launch DentalOS as Customer	✓	✓	✓	X
View Audit Log	✓	✓	✓	X
Migrate Users	✓	X	X	X
Marketing Tab - Manage Agents	✓	X	X	✓

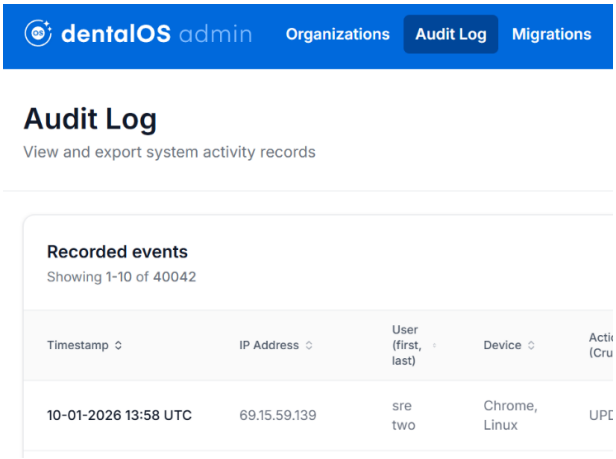
NOTE: There is no flag for internal accounts in DentalOS, meaning the system cannot differentiate whether a PGID is for an internal team or external customers.

Internal team members migrating their accounts to DentalOS should mark their accounts as internal when entering the organization name (e.g. INTERNAL: Duke Dentistry).

Audit log

The internal console for Planet DDS teams permits users to view and export system activity specific to **DentalOS Admin** via the **Audit Log**. These records can be accessed via the **Audit Log** tab in **DentalOS Admin.**

The internal audit log for **DentalOS Admin** looks slightly different than what customers see.



Migrations

The **Migrations** tab is used to onboard existing users and locations within DentalOS. Implementation Coordinators will handle this task.

Simply because an organization's information is available from DentalOS Admin, that does not mean the customer can utilize the DentalOS platform without error. A migration will transfer all the organization's data, including locations, customer accounts, and credentials.

The first step in migrating customers is to ensure organizational data accurately reflects the customer's present state. For this reason, validating each organization's information against Salesforce and assigning products to org groups is critical. Revisit Internal configuration for more context.

Follow the steps below to migrate an existing organization to DentalOS.

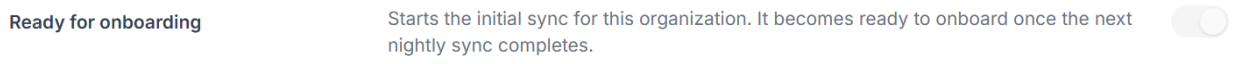
Step 1. Open **DentalOS Admin**.

Step 2. Go to the **Organizations** tab. Select the organization and remain on the **Organization details** tab.

Step 3. Click **Edit organization details** on the top right, and scroll down to the **Ready for onboarding** flag. Toggle on the flag to start a nightly sync that will create user accounts and locations in **DentalOS** based on the organization's existing product application data.

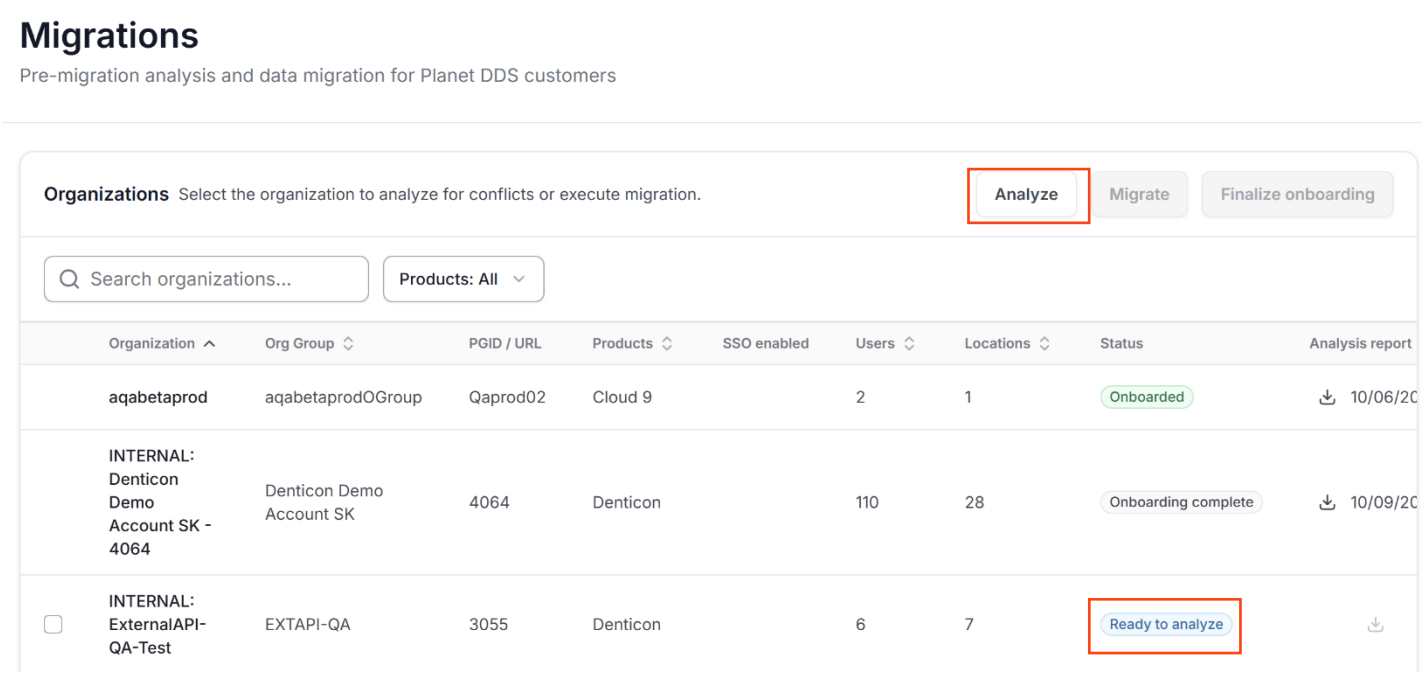
As this process occurs overnight, organizations cannot migrate until the following day after completing this step. If a migration is planned for a specific date, be mindful of this timing.

This step should only occur when products and organization information (e.g., PGID, org groups) are successfully linked.



Step 4. Navigate to the **Migrations** tab which displays the onboarding status of synced organizations. The organizations that have been synced most recently should appear under the **Status** field as **Ready to analyze**.

Step 5. In the **Ready to analyze** state, data has been retrieved from the product applications and can enter an analysis state via the **Analyze** button. Clicking this will cross-reference each user and location against the data that already exists in DentalOS.



Step 6. Once analyzed, an output file will materialize in the **Analysis report** field for download. The document gives a line-by-line breakdown of how locations and users will be added as a result of migration. It will also disclose whether migration is feasible at all for specified users and locations.

The outcome map linked here and in the appendix describe the documentation in more detail. Certain account issues will prevent the organization from migrating successfully.

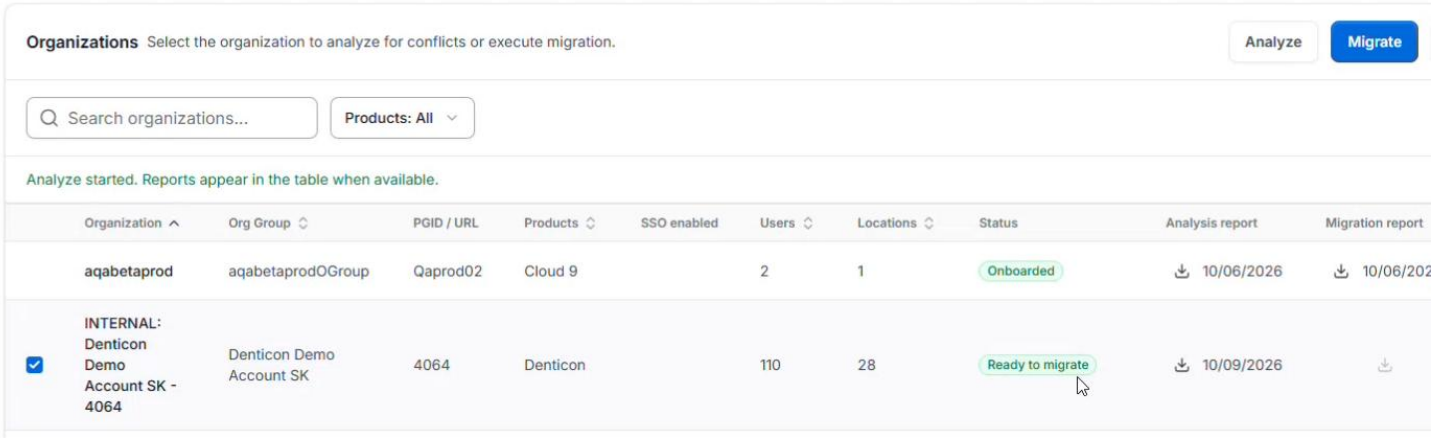
Migrations can still occur with conflicts, but the users and locations with identified issues may not. This may require further action from the customer or internal staff to resolve.

Step 7. Once the analysis report is available for download, the **Migrations** interface will also change the status of the organization. Unless there are any blocking issues identified in the report, the **Status** field will read **Ready to migrate**.

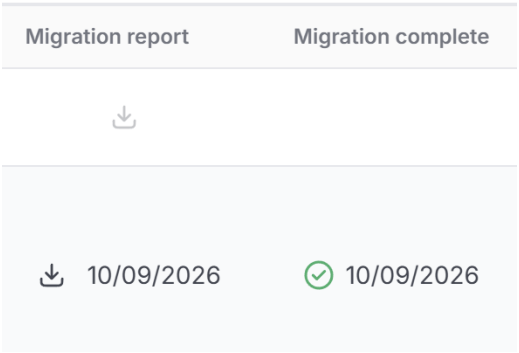
Selecting the account, then clicking **Migrate** will start the migration of data, regardless of any conflict. At this stage, users and locations are added in real-time into DentalOS.

Multiple accounts can be migrated at once.

NOTE: A migration alone does not alter end-user experience. Only clicking **Finalize Onboarding** will change the log-in experience for users.



Step 8. When the migration is complete, a migration report will populate in its associated field. The report contains similar data to that of the analysis report, but more robust.



Step 9. Select the organization and click **Finalize onboarding** to formally change the authentication route for users, meaning product access will only occur via DentalOS from this point onwards. The **Status** field will change to **Onboarding complete** as a result.

This process is covered in the resources link mentioned above under **Existing customers — basic onboarding**.

NOTES:

- If the migration fails or issues prevent the customer from going live, contact Alanna Innes. Engineering can roll back the migration if needed. Rollbacks are expected to be rare.
- If there is a genuine discrepancy where a user or location has not been migrated but should be, best practice is to add their data after onboarding the organization to DentalOS.
- For usernames that are not unique, DentalOS automatically appends the PGID to the username. For example, testuser becomes testuser_5000.

Organization management

Besides editing organization details (demonstrated in Editing an organization), DentalOS Admin allows internal teams to manage customers directly on behalf of the organization.

Much of the process for managing an organization is detailed above in Internal configuration. This is the process of selecting an organization from the **Organizations** tab, then clicking the **Launch DentalOS** button.

From this point onwards, the user will be operating in DentalOS rather than DentalOS Admin and acting as an administrator within the selected organization.

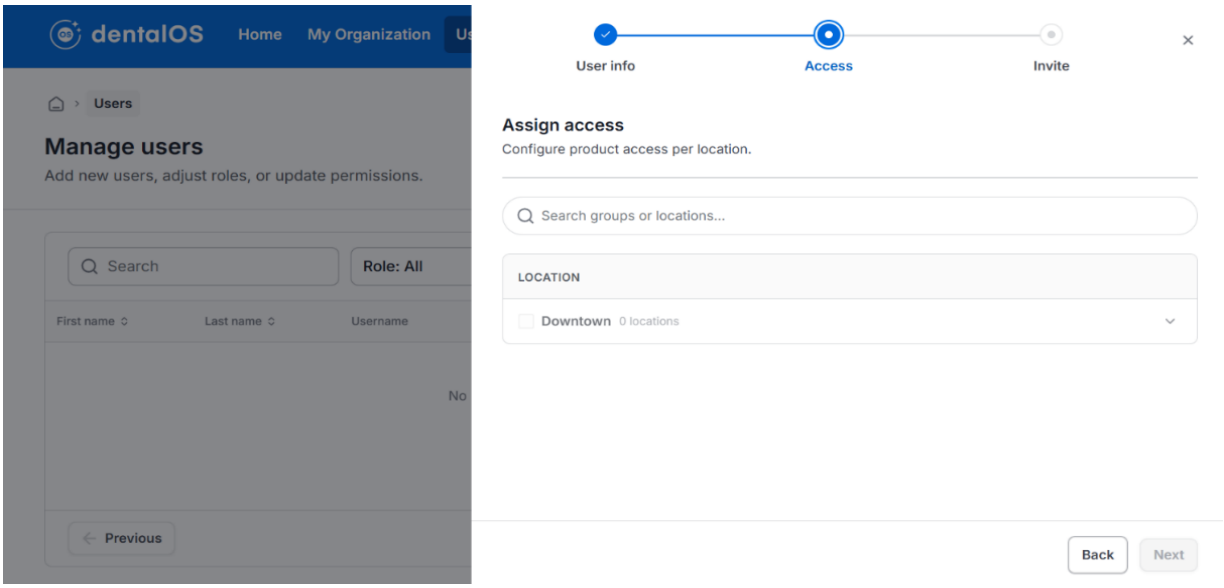
The other major use cases of this guide illustrate the actions organization administrators can take within DentalOS.

User management

Via the **Users** tab in DentalOS, an organization can create, delete, and manage users. Users cannot be created or deleted directly in a PMS (e.g., Cloud 9 or Denticon).

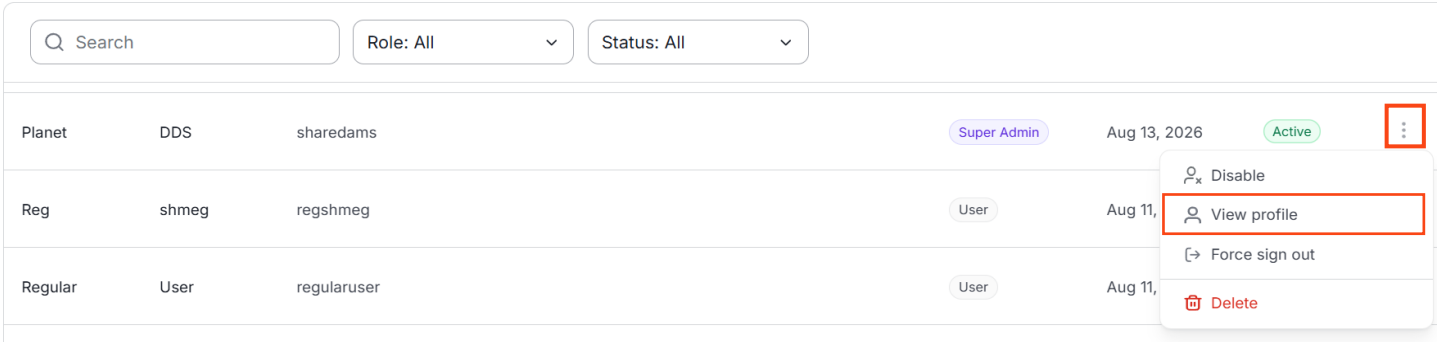
To create a user, customers should follow steps 2-10 from Creating super admins above, disregarding the instruction to select **Super admin**. Instead, they should select the user role most applicable to the circumstances.

If **Super admin** is not selected, at step 4, the user will be asked to select which locations per product the user should have access to.



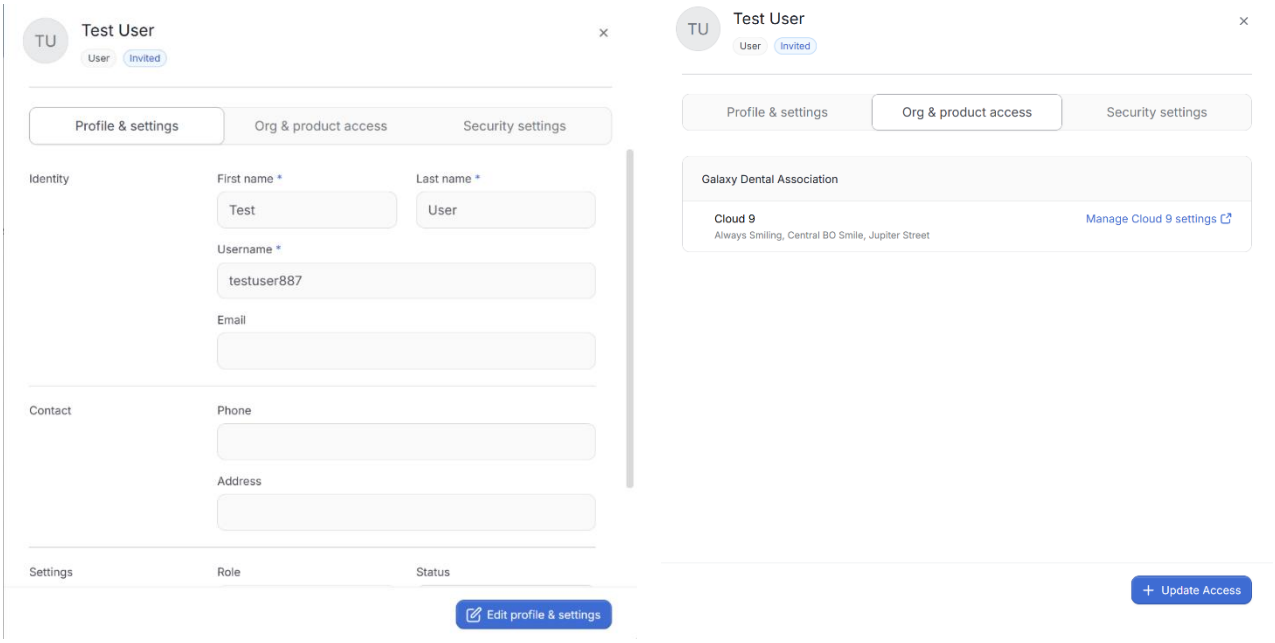
Admins can manager users from the **Users** tab. Use the ellipsis highlighted below to view, disable, delete, or force sign out for a given user. Invites can also be resent to inactive accounts by clicking this icon.

Disabling an account will not kick the user from any active sessions in a product, but it will prevent them from logging in at the next attempt. Force sign-out will kick users from active sessions.



By clicking the ellipsis and then **View profile**, the user can access **Profile & settings**, **Org & product access**, and **Security settings**.

The **Profile & settings** tab permits the admin to edit the user's personal details, contact information, and role privileges. Through **Org & product access**, customer admins can add or remove access to locations for a user.



Below is a quick reference of user role options.

User roles	Description
Super admin	Full administrative rights across the organization with the ability to customize which settings other users see on the dashboard; used for the very first user and any customer-side IT/office administrator
Group admin	Administrative rights scoped to specific org group/location groupings rather than the whole organization but with no privileges for managing security or dashboard settings; useful for multi-location customers who want local managers
User	Standard end-user access (front desk staff, clinicians, etc.) with permissions defined by whatever the admins configure; no organization-wide administrative rights or ability to see org groups

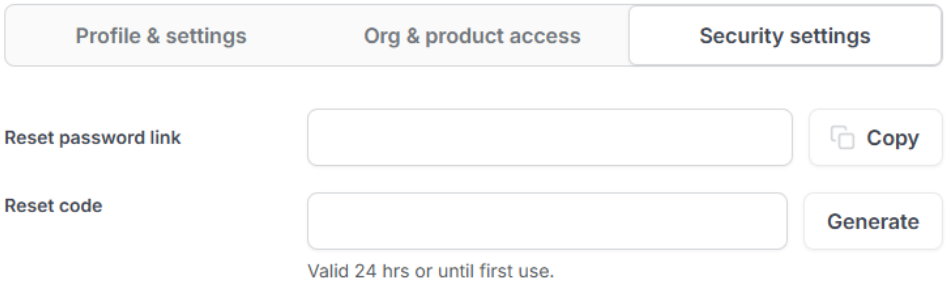
These roles specifically relate to DentalOS and do not implicate permissions within product applications such as Denticon.

NOTE: DentalOS does not support bulk updates of users.

Account recovery

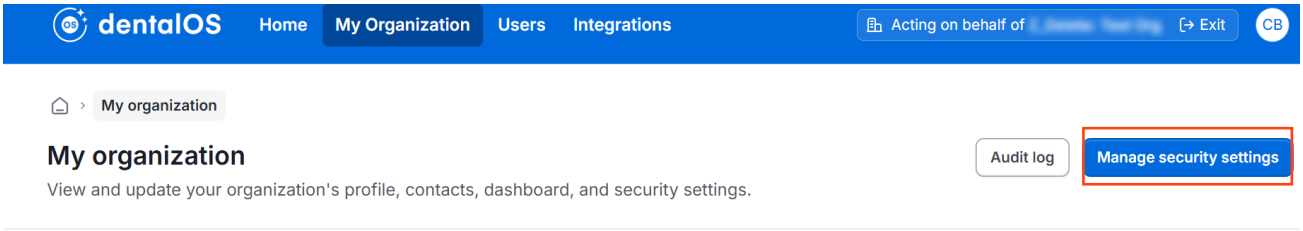
Via **Users → View profile → Security settings**, administrative accounts can generate a **Reset code** and a **Reset password link**.

When **Self-service password reset** is disabled, this is the only way to reset a user password. View the Security policy management section of this resource for more information.

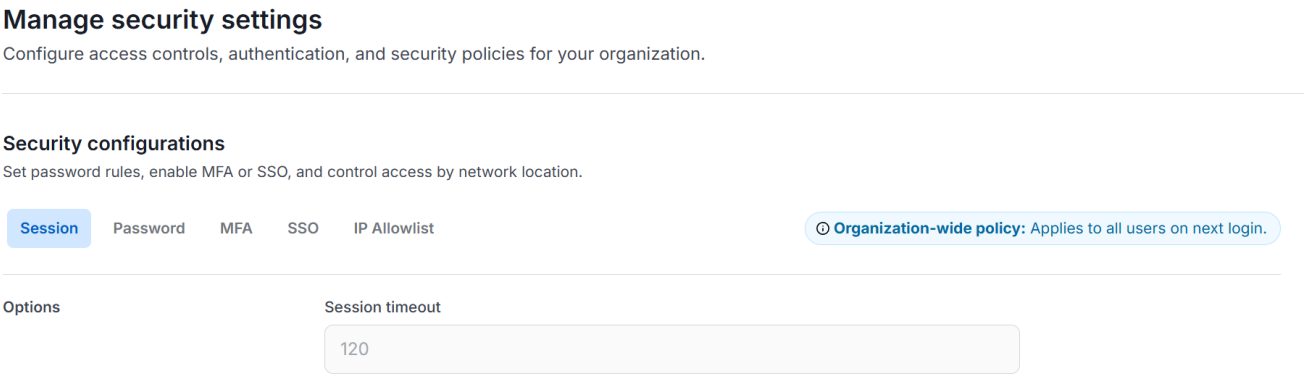


Security policy management

Super admins can configure security settings such as MFA, SSO, and an IP Allowlist organization wide. The user must select **Manage security settings** to access these features.



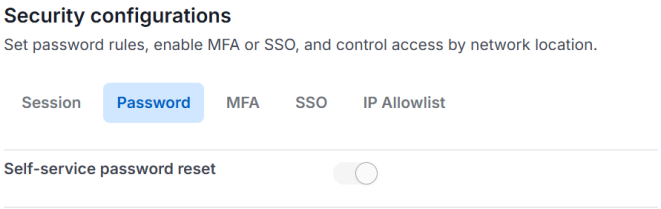
The first security setting is the session timeout, which is defaulted to 120 minutes and cannot be configured.



Password rules are also not customizable. However, if **Self-service password reset** is enabled, users will be able to click **Forgot password** on the sign-in page.

Alternatively, once signed into **DentalOS**, users can click their profile icon in the top right, revealing an option to reset their password. Users may also change their password by clicking their profile icon in **DentalOS**. Usernames cannot be changed.

If **Self-service password reset** is toggled off, only the user administrator can reset passwords.

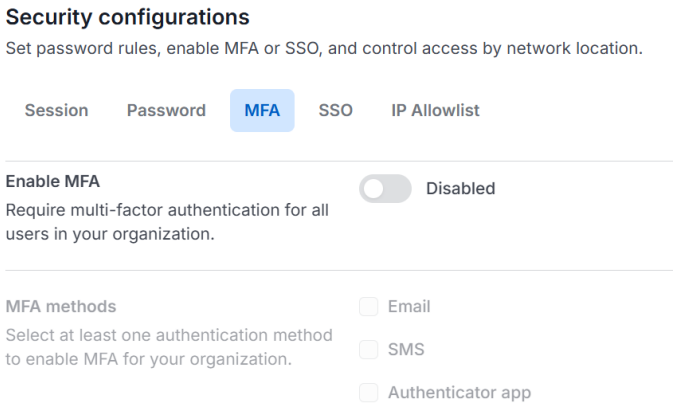


User authentication

DentalOS supports a unified login and logout experience with multiple authentication options.

- Multi-factor authentication (MFA): Adds an additional verification using the method selected by the super admin
- Microsoft Entra ID single sign-on (SSO): Allows users to sign in to DentalOS using their organization-managed Microsoft credentials, reducing the need for a separate username and password

MFA can be enabled with email, SMS, or authenticator app. If a customer enables MFA with email, all the users within the organization must have an email on file. Otherwise, they will not be able to sign in.

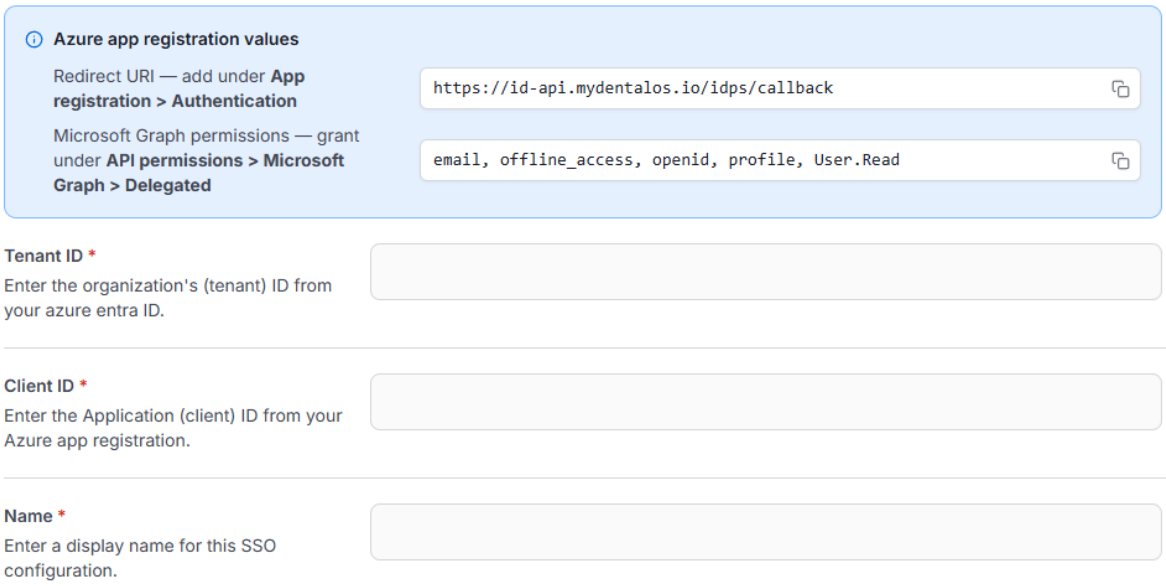


Similarly, if a customer enables MFA for SMS, every user must have a phone number on record to enroll in multi-factor authentication through this method.

The authenticator app selection will send users a QR code and prompt them to set up this MFA method on their next DentalOS sign-in. Users will be required to install Microsoft Authenticator on their devices. The app sends push notifications with relevant information to secure the user's subsequent sign-ins.

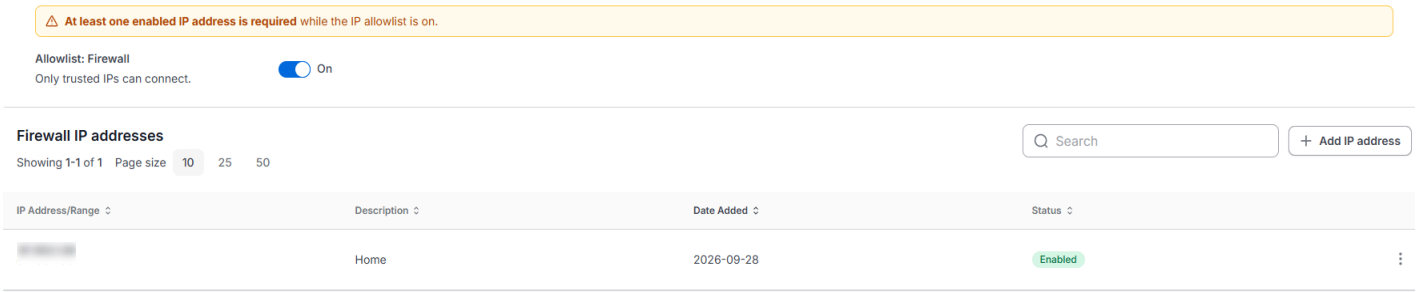
The SSO tab shows the Azure app registration values customers need to set up SSO with their Entra tenant. Below, the customers must enter the values associated with their Entra tenant. Once enabled, SSO will apply at users' next log-in.

NOTE: Entra IDs cannot be used for more granular access management. SSO is used only for sign-in. Creating a new Entra user will not create a synced DentalOS account. Customers must add users manually, ensuring the username and Entra ID email are the same.



IP allowlist

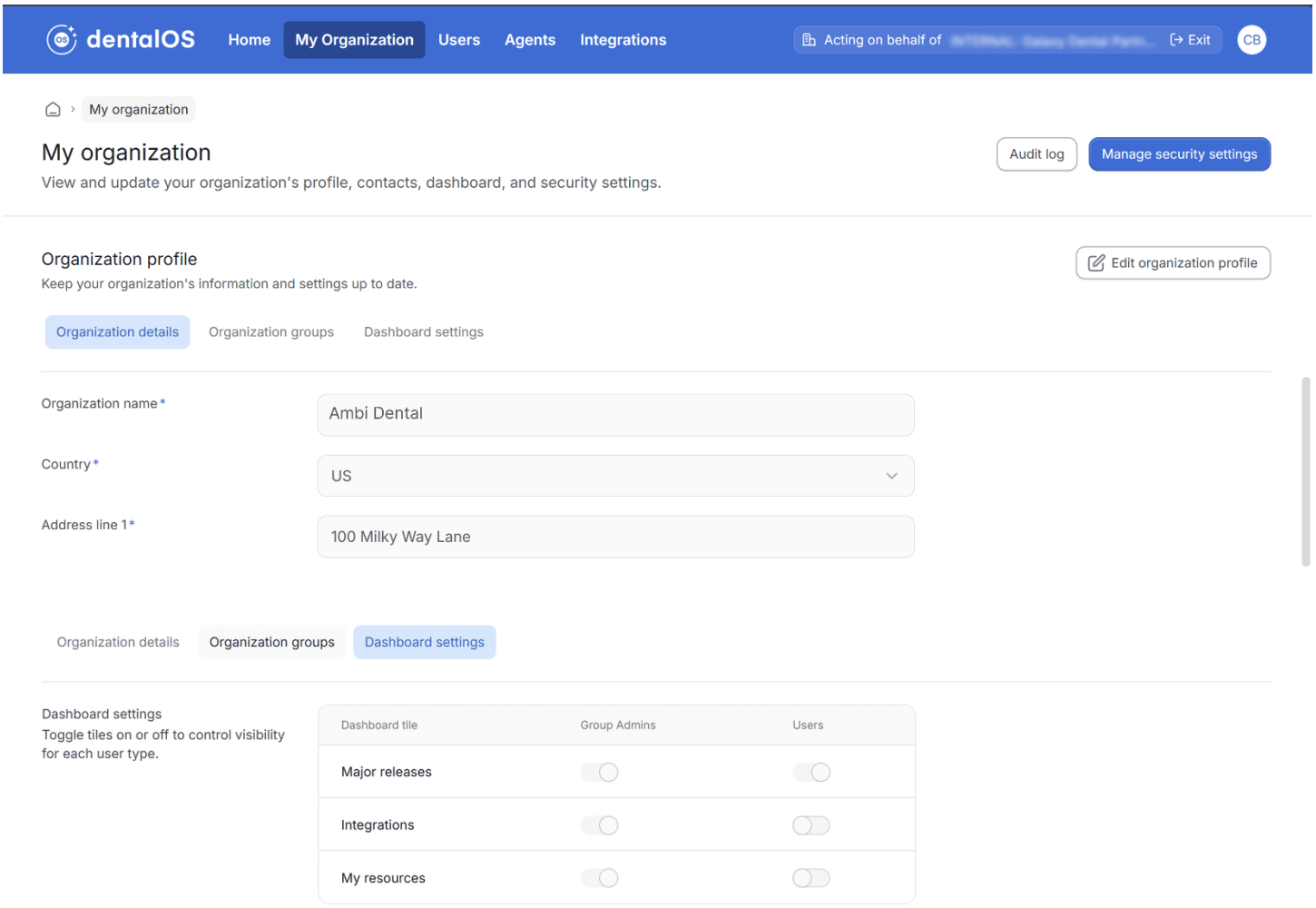
The last security configuration available to users is the **IP Allowlist**. This feature allows organizations to restrict **DentalOS** access to approved IP addresses, helping prevent sign-ins from unauthorized networks.



Customers may want to include the public IP address for a corporate office or another approved network like a third-party vendor. When the firewall is enabled, the IP address will be evaluated against the allowlist. If the IP address is not on the allowlist, users connecting through that address cannot access **DentalOS** or any of the connected tools.

Organization administration

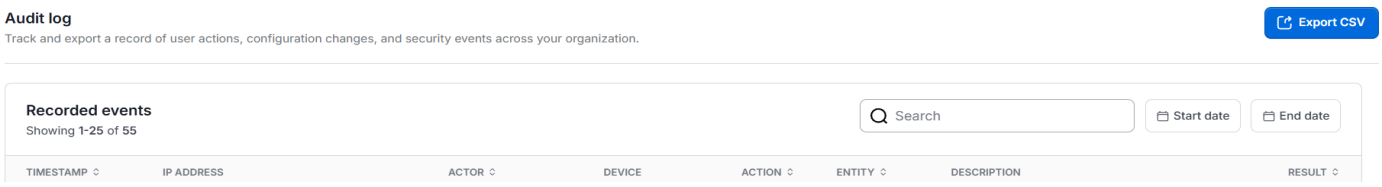
Customer administrators can update key settings that shape how the organization is structured and how users experience DentalOS through the **My Organization** tab.



While internal teams initially manage this information, organizations can change details after the fact. This is also where super admins can edit dashboard settings for users within their organization.

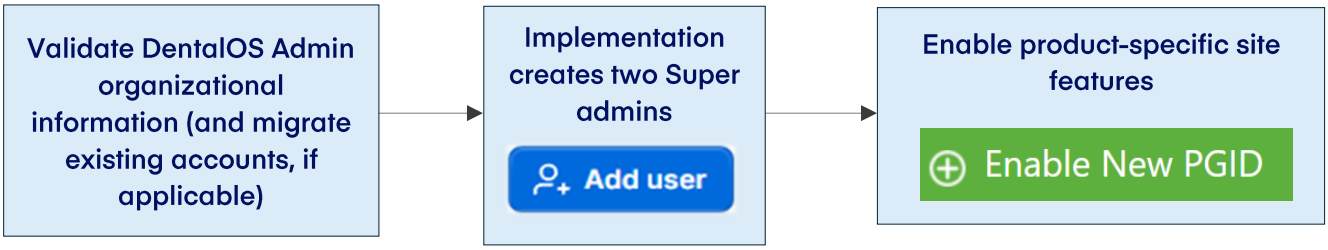
Audit log

The audit log enables customer administrators to view and track system activity that occurs within their organization, specific to **DentalOS**. To access the audit log, go to the **DentalOS** website, select **My Organization**, then **Audit log.**

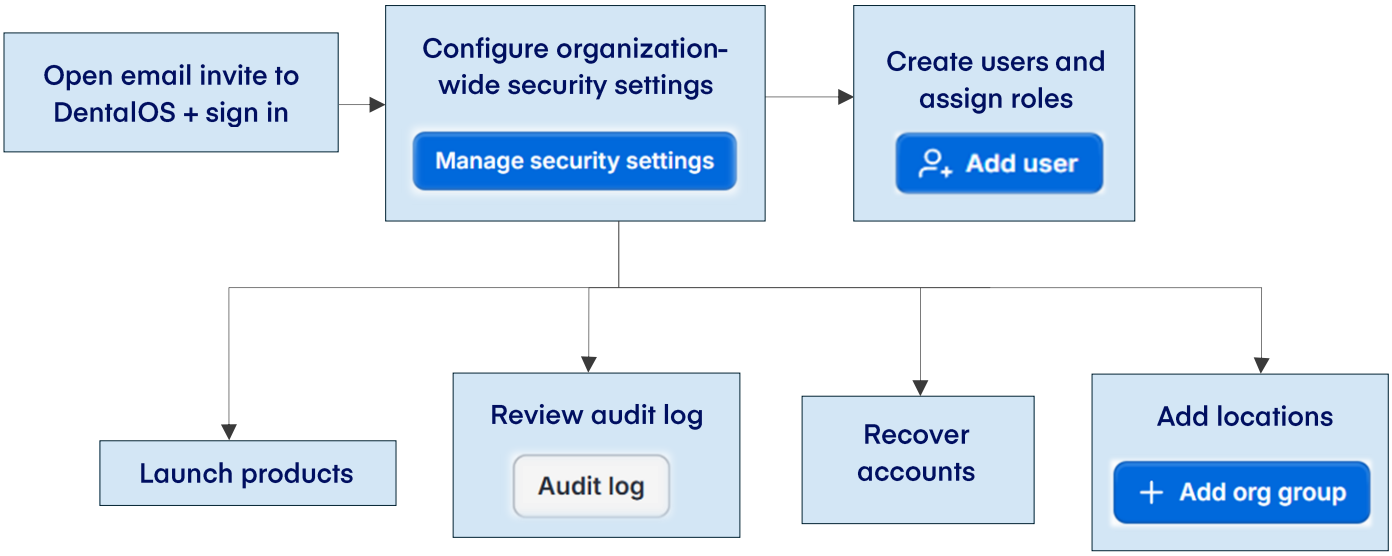


General workflows

Customer onboarding



Super admin tasks



05. Troubleshooting

User cannot sign in to DentalOS

- Confirm the user completed the email invitation or one-time setup process.
- Confirm the Super admin added the relevant user with accurate information.

User did not receive an invitation email

- Confirm the user was created with an email address.
- If the user was created without an email address, confirm the user received a generated setup link and code.
- If an emailed invitation expired, resend it from the **Users** tab in **DentalOS**. Email invitations expire after 24 hours.

User cannot see or launch an expected product

- Confirm the product is enabled for the organization according to the customer contract.
- Confirm the product is assigned to the correct organization group.
- Confirm the user has been assigned access to the product and applicable locations.

- Super admins should inherit access to all locations automatically, but location access may not propagate immediately. If a newly created Super admin is missing locations, check for delayed propagation before escalating the issue.
- Verify that the required product account information is correct, such as a Denticon PGID or Cloud 9 subdomain.
- Confirm granular permissions were configured in the applicable core product.
- For Apteryx/XV Web and other integrations that use silent single sign-on, confirm that browser pop-ups are allowed. The OIDC sign-in flow depends on a pop-up window, so blocked pop-ups can prevent sign-in without displaying an obvious error.

User has DentalOS access but insufficient permissions inside Denticon or Cloud 9

DentalOS creates the connected product account, but it does not replace granular permissions configured within each core product.

- In Denticon, go to **Setup → Security**, locate the user, and confirm the appropriate user groups and user settings.
- In Cloud 9, go to **Edit → Setup → Employees**, locate the user, and confirm the appropriate permissions.
- Confirm the user was assigned to the correct product and locations in DentalOS. If the user has insufficient permissions or lands in the wrong Denticon office, confirm that the correct home office and permissions are also assigned inside Denticon.

Multi-factor authentication or Entra ID single sign-on is unavailable

- Confirm the applicable MFA or SSO feature flag is enabled at the product level.
- For Entra ID SSO, confirm the user's DentalOS username and email address are the same.
- For MFA, confirm all users have included credentials for email or SMS, depending on the selected authentication method.

Frequently asked questions

Why do I not see a product or location that I need?

Your role, product access, and location assignments determine what appears in DentalOS. Contact your administrator to confirm that you were assigned to the correct product and location.

Why can't I add new locations in Denticon?

Locations must be added via DentalOS and can no longer be added in Denticon.

What happens when a DentalOS account is disabled or in the event of a force-sign-out?

You will be prevented from signing in again. An administrator may also use force sign-out to end your active session in a connected product.

How do I resend an invite?

To resend an invite, open **DentalOS Admin**, select the user's organization via the **Organizations** tab, and launch **DentalOS** on behalf of the organization.

Select **Users**, search for the relevant Super admin, click the ellipsis menu to the far right of the user's name, then select **Resend invite.**

Manual setups can also occur at a later point via this step.

Can customers create their own org groups?

No, org groups can only be created internally through **DentalOS Admin.**

06. Appendix

Other resources

Resource	Description	Site
Video Walkthrough: DentalOS Admin	Describes how to add an organization, enable products, and create org groups	DentalOS Admin INTERNAL Demo (Tella)
Onboarding Guide	A short reference of internal implementation activities	DentalOS Admin User Guide
Video Walkthrough: Client Experience	In-depth overview of what is available to customers	DentalOS INTERNAL Demo (Tella)
DentalOS Admin + Salesforce	A video walkthrough for validating customer information in DentalOS Admin against Salesforce	DentalOSSaleforce.mp4
DentalOS Admin + Salesforce: Account & Product Setup Guide	A step-by-step guide for validating customer information in DentalOS Admin against Salesforce	DentalOS_Salesforce_User_Guide.docx
Onboarding Resources	Onboarding resources covering eligibility, username conflicts, customer journeys, analysis, feedback, and dashboard tracking	Onboarding links

Revisions

Version No.	Last modified	Major change	Author
1	10/05/2026	Initial build	Cordenne Brewster
2	10/11/2026	Removed section on adding an organization; added revision control	Cordenne Brewster
3	10/20/2026	Revised use cases to include DentalOS Admin and migration information; final updates based on feedback from product owners	Cordenne Brewster